CLAIMS

What is claimed is:

1. A method of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device, the method comprising:

generating a fingerprint within the FPGA, the fingerprint representing an inherent manufacturing process characteristic unique to the FPGA;

transmitting encrypted configuration data from the storage device to the FPGA; and

decrypting the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data.

2. The method of Claim 1, further comprising: configuring the FPGA using the configuration data.

3. The method of Claim 2, further comprising:

transmitting the fingerprint from the FPGA to an encryption circuit;

encrypting the configuration data using the fingerprint as an encryption key; and

storing the encrypted configuration data in the storage device.

4. The method of Claim 1, wherein the fingerprint is generated during power-up of the FPGA.

5. The method of Claim 1, wherein generating the fingerprint comprises:

measuring propagation delays for a plurality of circuit elements on the FPGA; and

combining the propagation delays to generate the fingerprint.

6. The method of Claim 5, wherein generating the fingerprint further comprises:

counting the number of oscillations of an oscillator on the FPGA during a predetermined time interval.

7. The method of Claim 6, wherein the oscillator comprises a configurable logic block of the FPGA.

8. The method of Claim 5, wherein generating the fingerprint further comprises:

counting the number of oscillations of a first oscillator on the FPGA during a predetermined time interval;

counting the number of oscillations of a second oscillator on the FPGA during the predetermined time interval; and

generating a ratio between the resultant first and second oscillator counts that is used as the fingerprint.

9. The method of Claim 1, wherein generating the fingerprint comprises:

providing a plurality of line segments on the FPGA;

determining whether a width of each line segment is less than a predetermined value; and

means for generating, for each line segment, a corresponding bit of the fingerprint in response to the determining step.

10. The method of Claim 1, wherein generating the fingerprint comprises:

using differences in transistor threshold voltages caused by manufacturing process variations to generate the fingerprint.

11. The method of Claim 10, wherein generating the fingerprint further comprises:

applying a read voltage to a plurality of transistor pairs;

determining, for each transistor pair, whether a first transistor or a second transistor of the pair turns on earlier;

generating, for each transistor pair, a corresponding bit of the fingerprint in response to the determining step.

12. A field programmable gate array (FPGA), comprising:

a plurality of configurable logic elements being programmable with configuration data to implement a desired circuit design;

a fingerprint element for generating a fingerprint representing inherent manufacturing process variations unique to the FPGA; and

a decryption circuit coupled to receive encrypted configuration data, the decryption circuit configured to decrypt the encrypted configuration data using the fingerprint as a decryption key to extract the configuration data.

13. The FPGA of Claim 12, further comprising:

a configuration circuit for configuring the configurable logic elements with the configuration data.

14. The FPGA of Claim 12, further comprising:

a storage device external to the FPGA, the storage device for storing the encrypted configuration data.

15. The FPGA of Claim 14, wherein the configuration data is encrypted using the fingerprint as an encryption key to generate the encrypted configuration data.

16. The FPGA of Claim 15, wherein the storage device includes an encryption circuit.

17. The FPGA of Claim 12, wherein the fingerprint element comprises:

a plurality of line segments on the FPGA; and

a sensing circuit, comprising:

means for determining whether each line width is less than a predetermined value; and

means for generating, for each line segment, a corresponding bit of the fingerprint in response to the determining step.

18. The FPGA of Claim 12, wherein the fingerprint element comprises:

a plurality of transistor pairs; and

a sensing circuit, comprising:

means for determining, for each transistor pair, whether a first transistor or a second transistor of the pair turns on earlier when a read voltage is applied thereto; and

means for generating, for each transistor pair, a corresponding bit of the fingerprint according to which transistor of the pair turns on earliest.

19. The FPGA of Claim 12, wherein the fingerprint element comprises:

a plurality of circuit elements; and

a sensing circuit, comprising:

means for measuring propagation delays for each of the plurality of circuit elements; and

means for combining the propagation delays to generate the fingerprint.

20. The FPGA of Claim 12, wherein the fingerprint element comprises:

an oscillator; and

a sensing circuit for counting the number of oscillations of the oscillator during a predetermined time interval.

21. The FPGA of Claim 20, wherein the oscillator comprises a configurable logic block.

22. The FPGA of Claim 12, wherein the fingerprint element comprises:

first and second oscillators; and

a sensing circuit, comprising:

means for counting the number of oscillations of the first and second oscillators during a predetermined time interval; and

means for generating a ratio between the resultant first and second binary oscillator count values, the ratio being used as the fingerprint.

23. An apparatus for programming a field programmable gate array (FPGA), comprising:

a storage device external to the FPGA, the storage device for storing encrypted configuration data and transmitting the encrypted configuration data to the FPGA;

a fingerprint element within the FPGA, the fingerprint element for generating a fingerprint representing an inherent manufacturing process variation unique to the FPGA;

a decryption circuit coupled to receive the encrypted configuration data, the decryption circuit

for decrypting the encrypted configuration data using the fingerprint as a decryption key to extract the configuration data; and

a plurality of configurable logic elements within the FPGA, the plurality of configurable logic elements being programmable with the configuration data to implement a desired circuit design.

24. The apparatus of Claim 23, further comprising:

a configuration circuit within the FPGA for configuring the configurable logic elements with the configuration data.

25. The apparatus of Claim 23, wherein the configuration data is encrypted using the fingerprint as an encryption key to generate the encrypted configuration data.

26. The apparatus of Claim 25, wherein the storage device includes an encryption circuit.

27. The apparatus of Claim 23, wherein the fingerprint element comprises:

a plurality of circuit elements; and

a sensing circuit, comprising:

means for measuring propagation delays for each of the plurality of circuit elements; and

means for combining the propagation delays to generate the fingerprint.

28. The apparatus of Claim 23, wherein the fingerprint element comprises:

a plurality of line segments; and

a sensing circuit, comprising:

means for determining whether each line width is less than a predetermined value; and

means for generating, for each line segment, a corresponding bit of the fingerprint in response to the determining step.

29. The apparatus of Claim 23, wherein the fingerprint element comprises:

a plurality of transistors pairs; and

a sensing circuit, comprising:

means for determining, for each transistor pair, whether a first transistor or a second transistor of the pair turns on earlier when a read voltage is applied thereto; and

means for generating, for each transistor pair, a fingerprint bit according to which transistor of the pair turns on earliest.

30. The apparatus of Claim 23, wherein the fingerprint element comprises:

an oscillator; and

a sensing circuit for counting the number of oscillations of the oscillator during a predetermined time interval.

31. The apparatus of Claim 30, wherein the oscillator comprises a configurable logic block.

32. The apparatus of Claim 23, wherein the fingerprint element comprises:

first and second oscillators; and

a sensing circuit, comprising:

means for counting the number of oscillations of the first and second oscillators during a predetermined time interval; and

means for generating a ratio between the resultant first and second binary oscillator count values, the ratio being used as the fingerprint.

33. A method of securing communication of configuration data between a field programmable gate array (FPGA) and an external storage device, the method comprising:

generating a fingerprint within the FPGA, the fingerprint representing an inherent manufacturing process characteristic unique to the FPGA;

receiving encrypted configuration data from the storage device by the FPGA; and

decrypting the encrypted configuration data in the FPGA using the fingerprint as a decryption key to extract the configuration data.

34. The method of Claim 33, further comprising:

configuring the FPGA using the configuration data.

35. The method of Claim 34, further comprising:

transmitting the fingerprint from the FPGA to an encryption circuit;

encrypting the configuration data using the fingerprint as an encryption key; and

storing the encrypted configuration data in the storage device.

36. The method of Claim 33, wherein the fingerprint is generated during power-up of the FPGA.

37. The method of Claim 33, wherein generating the fingerprint comprises:

measuring propagation delays for a plurality of circuit elements on the FPGA; and

combining the propagation delays to generate the fingerprint.

38. The method of Claim 37, wherein generating the fingerprint further comprises:

counting the number of oscillations of an oscillator on the FPGA during a predetermined time interval.

39. The method of Claim 38, wherein the oscillator comprises a configurable logic block of the FPGA.

40. The method of Claim 37, wherein generating the fingerprint further comprises:

counting the number of oscillations of a first oscillator on the FPGA during a predetermined time interval;

counting the number of oscillations of a second oscillator on the FPGA during the predetermined time interval; and

generating a ratio between the resultant first and second oscillator counts that is used as the fingerprint.

41. The method of Claim 33, wherein generating the fingerprint comprises:

providing a plurality of line segments on the FPGA;

determining whether a width of each line segment is less than a predetermined value; and

means for generating, for each line segment, a corresponding bit of the fingerprint in response to the determining step.

42. The method of Claim 33, wherein generating the fingerprint comprises:

using differences in transistor threshold voltages caused by manufacturing process variations to generate the fingerprint.

43. The method of Claim 42, wherein generating the fingerprint further comprises:

applying a read voltage to a plurality of transistor pairs;

determining, for each transistor pair, whether a first transistor or a second transistor of the pair turns on earlier;

generating, for each transistor pair, a corresponding bit of the fingerprint in response to the determining step.